

IN THE CLAIMS**Listing of Claims:**

- 1 1. (original) A method for ensuring a secure programming environment for a computer
2 system comprising the steps:
3 modifying a processor of said computer system to incorporate an S-latch, a first
4 state of said S-latch setting said processor in a secure state and a second state of said
5 S-latch setting said processor in a non-secure state;
6 writing a security code in an NVRAM coupled to said computer system;
7 reading said security code from said NVRAM;
8 setting said first and second state of said S-latch in response to states of said
9 security code; and
10 not accepting processor commands from an In Circuit Emulator (ICE) unit
11 coupled to said computer system when said S-latch is in said first state and accepting
12 processor commands from said ICE unit when said S-latch is in said second state.
- 1 2. (original) The method of claim 1, wherein said security code is read by boot block
2 code within a Basic Input Output System (BIOS) code of said computer system.
- 1 3. (original) The method of claim 2, wherein said S-latch is set by said boot block code
2 in response to reading said security code.
- 1 4. (original) The method of claim 2, wherein said boot block code is a first code
2 executed on each power up or system reset of said computer system.
- 1 5. (currently amended) The method of claim 1, wherein said security code is encrypted
2 when written into said NVRAM [[unit]].
- 1 6. (currently amended) The method of claim 1, wherein said security code is password
2 protected when written into said NVRAM [[unit]].
- 1 7. (original) The method of claim 2, wherein said BIOS code is executed if said boot
2 block code is able to authenticate said security code and said boot block code is able to

3 write to said S-latch if said security code corresponds to setting said first state of said
4 S-latch.

1 8. (original) The method of claim 2, wherein said BIOS code is not executed if said boot
2 block code is not able to authenticate said security code.

1 9. (original) The method of claim 2, wherein said BIOS code is not executed if said boot
2 block code is able to authenticate said security code and said boot block code is not able
3 to set a state of said S-latch.

1 10. (original) The method of claim 1, wherein said ICE unit is coupled to said computer
2 system on a system bus of said computer system.

1 11. (original) The method of claim 1, wherein said ICE unit is coupled to said computer
2 system on a JTAG scan chain bus.

1 12. (original) The method of claim 1, wherein said ICE unit is coupled to said computer
2 system in place of said modified processor.

1 13. (original) The method of claim 1, wherein a default said S-latch in said computer
2 system is set to a non-secure state.

1 14. (currently amended) A computer system comprising:
2 a central processing unit (CPU);
3 a random access memory (RAM);
4 non-volatile RAM (NVRAM);
5 a communications adapter coupled to a communication network;
6 an I/O adapter;
7 a bus system coupling said CPU to said NVRAM, said communications adapter,
8 said I/O adapter, and said RAM, wherein said CPU further comprises:

9 a modified processor with an S-latch, a first state of said S-latch setting said
10 modified processor in a secure state and a second state of said S-latch setting said
11 modified processor in a non-secure state;

12 first circuitry operable to receive and write a security code in said NVRAM;
13 second circuitry operable to read said security code from said NVRAM; ~~and~~
14 ~~circuitry~~ and operable to set said first and second state of said S-latch in response
15 to states of said security code;

16 wherein said modified processor accepts commands from an In Circuit Emulator
17 (ICE) unit coupled to said computer system when said S-latch is in said second state and
18 does not accept processor commands from said ICE unit when said S-latch is in said first
19 state.

1 15. (original) The computer system of claim 14, wherein said security code is read by
2 boot block circuitry within Basic Input Output System (BIOS) circuitry of said computer
3 system.

1 16. (original) The computer system of claim 15, wherein said S-latch is set by said boot
2 block circuitry in response to reading said security code.

1 17. (original) The computer system of claim 15, wherein said boot block circuitry reads
2 said security code as a first operation on each power up or system reset of said computer
3 system.

1 18. (currently amended) The computer system of claim 14, wherein said security code is
2 encrypted when written into said NVRAM [[unit]].

1 19. (currently amended) The computer system of claim 14, wherein said security code is
2 pass word protected when written into said NVRAM [[unit]].

1 20. (original) The computer system of claim 15, wherein said BIOS circuitry is enabled
2 if said boot block code is able to authenticate said security code and said boot block code

3 is able to write to said S-latch if said security code corresponds to setting said first state
4 of said S-latch.

1 21. (original) The computer system of claim 15, wherein said BIOS circuitry is disabled
2 if said boot block is not able to authenticate said security code.

1 22. (original) The computer system of claim 15, wherein said BIOS circuitry is disabled
2 if said boot block circuitry is not able to set said S-latch into a state.

1 23. (original) The computer system of claim 14, wherein said ICE unit is coupled to said
2 computer system on a system bus of said computer system.

1 24. (original) The computer system of claim 14, wherein said ICE unit is coupled to said
2 computer system on a JTAG scan chain bus.

1 25. (original) The computer system of claim 14, wherein said ICE unit is coupled to said
2 computer system in place of said modified processor.

1 26. (original) The computer system of claim 14, wherein a default said S-latch in said
2 computer system is set to a non-secure state.